ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter
Capitolo di Roma

Newsletter

ANNO 2023 | N. 2 | FEBBRAIO

ISACA (Information Systems Audit and Control Association)

L'ISACA, (Information Systems Audit and Control Association), ha 160.296 associati in oltre 188 nazioni (dato aggiornato al 31 ottobre 2022) ed è l'organizzazione leader nella IT Governance, Security, Controllo ed Assurance. Fondata nel 1969, ISACA promuove conferenze internazionali, pubblica riviste di aggiornamento, sviluppa standard di Audit & Controllo e amministra le certificazioni professionali CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager), CGEIT (Certified in the Governance of Enterprise IT), CRISC (Certified in Risk and Information Systems Control) e CDPSE (Certified Data Protection Solutions Engineer) . I professionisti certificati CISA (dal 1978) sono più di 99500, mentre i CISM (dal 2002) risultano a quota 21000. Le certificazioni CGEIT (introdotta nel 2007) e CRISC (introdotta nel 2010) sono rispettivamente a quota 5400 e 16000.

EDITORIALE

Chat GPT, OPEN AI
e le considerazioni sulla sicurezza informatica e su quella per l'individuo

Da qualche tempo tutti sono alle prese con gli interrogatori ai sistemi di OPEN AI specialmente quello noto con il nome di CHAT GPT. Se sia per simulare un test di Turing o se sia per sentirsi parte della folta comunità che si fa una propria opinione su questi strumenti, nessuno sembra resistere al fascino di "chattare" con un algoritmo per verificarne le capacità, per testarne la prontezza e la qualità delle risposte, per cercare di provare che così intelligente non è, o per svago, curiosità, per capire come funzioni, sentirsi parte dell'ultimo trend…

Ma di cosa si tratta davvero e che implicazioni di sicurezza potrebbero esserci nell'uso di un algoritmo di Chat GPT? La domanda non ha molto senso se non ci chiediamo prima "sicuro rispetto a cosa e rispetto a quale ambito di applicazione?"

Andiamo con ordine. Per iniziare è bene chiarire che Chat GPT è definito dall'organizzazione OPEN AI che l'ha concretizzato, come un modello che interagisce in modo conversazionale. Il formato del dialogo abilita l'algoritmo nella risposta a domande, contestare premesse errate e rifiutare richieste inappropriate o ammettere i propri errori, ma è anche capace di fornire una risposta dettagliata ad una istruzione fornita da "Prompt dei comando". L'organizzazione no profit che ha generato questo modello di Intelligenza Artificiale si chiama OpenAI ed è un laboratorio di ricerca americano sull'intelligenza artificiale (AI o IA) costituito nel 2015 dalla OpenAI Incorporated (OpenAI Inc.) senza scopo di lucro e dalla sua società controllata che invece è a scopo di lucro, OpenAI Limited Partnership (OpenAI LP). Dalla sua fondazione OpenAI conduce ricerche sull'IA con l'intenzione dichiarata di promuovere e sviluppare un'AI amichevole. I sistemi OpenAI girano sul quinto supercomputer più potente al mondo. (Fonte sito Open AI). I diversi progetti in cui sono adottati algoritmi di intelligenza artificiale spaziano dalle capacità di dialogo (Chat GPT), alla produzione di immagini a partire da descrizioni in linguaggio naturale (progetto DALL E2), dalla produzione di codice a partire dal linguaggio naturale (Open AI Codex) alla produzione di musica e canto (livello rudimentale (Progetto Jukebox).

In relazione alla domanda sulla sicurezza, posta poche righe fa, vale la pena segnalare come nel 2018 gli stessi ricercatori di OpenAI si siano posti il problema di come una AI potesse essere usata in modo malevolo (Malicious use of AI n.d.r.), al fine di poter porre rimedio a questa eventualità. Per loro stessa ammissione e preoccupazione di un uso duale di questa tecnologia, dichiararono apertamente l'ovvia verità tautologica applicabile ad ogni tecnologia: "l'intelligenza artificiale è una tecnologia capace di applicazioni immensamente positive e immensamente negative" (fu vero per la dinamite e per la scissione dell'atomo per citare due esempi noti a tutti n.d.r.). La buona notizia è che i ricercatori fin dal 2018 hanno voluto ispirarsi ai principi della Cybersecurity (perlomeno nelle loro dichiarazioni n.d.r.) segnalando come l'utilizzo di pratiche di "red teaming" per sovvertire i sistemi, di previsione delle minacce prima che si manifestino e di scoperta di vulnerabilità nei sistemi di AI, li abbiano guidati rispettivamente per intervenire nella difesa e nel patching. Ma purtroppo oggi non abbiamo strumenti per valutare se quelle azioni di "fortificazione" abbiano funzionato completamente o solo parzialmente e temporaneamente. L'esperienza ci insegna purtroppo che il codice digitale è "sicuro" e "al sicuro" solo fino a quando non si manifesta un soggetto capace di

ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.

produrre un attacco con successo su quel codice. La brutta notizia è che una risposta definitiva all'uso malevolo delle AI non è stata data nemmeno da OpenAI, che anzi segnala casistiche di esempio, sulle quali è disposta a ragionare con la community tecnologica e politica, ma sulle quali non è in grado di agire da sola: reti neurali e tecniche di "fuzzing" usate per creare virus informatici con capacità di generazione automatica di exploit, attori malintenzionati capaci di violare un robot delle pulizie in modo che consegni un carico utile di esplosivi a un soggetto target, o come Stati canaglia che utilizzano sistemi di sorveglianza potenziati dall'AI per arrestare preventivamente le persone che si adattano a un profilo di rischio predittivo…. e così via.
Quindi il problema è lungi dall'essere risolto perlomeno da OpenAI. Ma fortunatamente la community scientifica è ampia come è ampia la community dedicata alla sicurezza. In particolare il gruppo di standardizzazione ETSI dedicato alla sicurezza dell'intelligenza artificiale (Industry Specification Group – Securing Artificial Intelligence) ha rilasciato uno specifico paper sulla sicurezza dell'IA già nel 2021: "*Securing Artificial Intelligence (SAI)*" . più di recente è l'intervento normativo della UE ad aver segnato il passo dell'uso sicuro delle AI. Infatti l'*Artificial Intelligence ACT*, mira proprio a bilanciare l'uso delle AI fra i "*benefici socio-economici dell'IA e i rischi o le conseguenze negative per gli individui o la società…. e per delineare un approccio europeo sulle implicazioni umane ed etiche dell'IA.*" Nel documento si legge che l'impostazione della proposta "*stabilisce norme armonizzate per lo sviluppo, l'immissione sul mercato e l'uso dei sistemi di IA nell'Unione secondo un approccio proporzionato basato sul rischio. Propone un'unica definizione di IA a prova di futuro. Alcune pratiche di IA particolarmente dannose sono vietate in quanto contrarie ai valori dell'Unione, mentre sono proposte restrizioni e salvaguardie specifiche in relazione a determinati usi di sistemi di identificazione biometrica remota a fini di contrasto. La proposta stabilisce una solida metodologia di rischio per definire i sistemi di IA "ad alto rischio" che comportano rischi significativi per la salute e la sicurezza o per i diritti fondamentali delle persone. Tali sistemi di IA dovranno rispettare una serie di requisiti orizzontali obbligatori per un'IA affidabile e seguire le procedure di valutazione della conformità prima che tali sistemi possano essere immessi sul mercato dell'Unione*".
Parallelamente alle norme e regole la ricerca non si è fermata e si va affermando l'AI Trust, Risk and Security Management (*AI Trism*), un'area di ricerca che cerca di garantire che i sistemi di Intelligenza artificiale siano sicuri e affidabili e che i rischi associati al loro utilizzo siano ridotti al minimo. (Per approfondire si veda la *pagina Gartner* dedicata al tema).
Tutto risolto quindi fra norme e ambiti di ricerca? Ovviamente no, perché il resto sta a noi. Come esseri umani "senzienti" abbiamo il diritto/dovere di sapere, per imparare a dubitare e a capire quando e come affidarci o meno ad una tecnologia, non perché decida per noi, ma perché ci supporti nelle decisioni da prendere, non per arrenderci ad essa, ma per vivere meglio grazie ad essa. D'altra parte, il progresso tecnologico ci ha permesso di evolvere dalla primitiva "clava", ma è sempre la nostra mano che deve effettuare la prima mossa, e che sia un gesto di polso per muovere la clava o che sia un "click", dovrebbe sempre essere un gesto pienamente consapevole e responsabile.

Alessia Valentini
Cyber security consultant, CISA

NOVITA' DAL CAPITOLO

ISACA Sistemi informativi: averne fiducia e trarne valore Rome Chapter

ACCORDO

Istituto Italiano di Project Management

È stato sottoscritto un accordo tra **ISACA Roma** e l'**Istituto Italiano di Project Management® (ISIPM)**, con il quale le due associazioni intendono promuovere e sviluppare un processo di collaborazione, nelle aree culturali di comune interesse di "Project Management" e ICT Security Management, attraverso l'organizzazione e la realizzazione di attività congiunte, al fine di promuovere i principi e le tecniche professionali.

Informiamo i Soci e i followers di ISACAROMA che stiamo proseguendo con lo svolgimento di eventi on-line. Le modalità di informazione sono le consuete mail di annuncio/invito spedite ai contatti della nostra mailing-list che coincide con la diffusione della Newsletter. Per iscriversi alla mailing list è sufficiente inviare una mail con oggetto SUBSCRIBE a *eventi@isacaroma.it*.
Vi terremo informati su eventuali eventi in presenza, per il momento vi auguriamo buona lettura!

ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.

EVENTI PASSATI

VENERDÌ 27 GENNAIO 2023 15:00-17:00 (2 CPE)

"LA CORSA VERSO NUOVI MONDI E LA CYBERSECURITY"

L'occasione di questo webinar nasce dal sempre maggior rilevo delle esplorazioni spaziali e dalle prospettive di crescita del settore a breve e a medio termine. Lo studio e l'esplorazione dei corpi celesti nel nostro sistema solare hanno condotto all'individuazione di possibili destinazioni d'interesse per le attività dell'uomo; verso le quali effettuare i primi passi al di fuori del pianeta Terra. Si tratta dell'individuazione di obiettivi, viaggi su pianeti del sistema solare, che richiedono la soluzione di problematiche molto complesse sia per raggiungerli che per abitarli per tempi più o meno lunghi. I fattori abilitanti sono rappresentati da tecnologie in grado di rispondere agli elevatissimi requisiti di affidabilità e resilienza richiesti per tali missioni spaziali. Tra queste tecnologie c'è sicuramente l'ICT nella doppia accezione di informatica e telecomunicazioni e quindi ecco entrare in campo anche le esigenze di cybersecurity, resilienza, ecc. Il webinar è l'occasione per uno sguardo panoramico su un possibile prossimo futuro in un'ottica di interdisciplinarità.

Relatori:
Gen. B.A. (c) Alberto Traballesi
In servizio presso l'Aeronautica Militare Italiana dal 1958 al 1995, ha lasciato il servizio attivo con il grado di Generale di Brigata Aerea. Sino al 2013 ha servito come esperto presso la Presidenza del Consiglio dei Ministri. Laureato in Matematica, Ingegneria elettronica e Scienze Aeronautiche. Attualmente è parte attiva in ricerche sulla protezione delle IC e sulle tematiche spaziali. È vicepresidente AIIC.
Ing. Roberto Sommma
Entrato in Selenia (oggi Thales Alenia Space) nel 1970 subito dopo la laurea in Ingegneria Elettronica, si è occupato fino al 1980 di Affidabilità dei Sistemi Spaziali. Gli è stata quindi affidata la responsabilità dello sviluppo de settore Telerilevamento, nel quale ha varato e diretto lo sviluppo dei radar spaziali. Dirigente dal 1985, nel 1991 ha avuto la direzione operativa della nuova Divisione Telerilevamento. In pensione a fine 2007, è rimasto in azienda fino al 2014 come Senior Advisor dell'Amministratore Delegato

La documentazione degli eventi passati è disponibile sul sito www.isacaroma.it

PROSSIMI EVENTI

ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.

VENERDÌ 24 MARZO 2023 15:00-17:00 (2 CPE)

"L'IMPORTANZA DELLA FORMAZIONE NELLA PROTEZIONE DEI DATI PERSONALI. Un esempio di formazione per la filiale bancaria"

L'obbligo di formazione (artt. 29 e 32 del GDPR) delle persone autorizzate al trattamento riveste, come peraltro nella previgente normativa, grande importanza nella protezione dei dati personali ed è posta oggi anche sotto la sorveglianza del DPO [art. 39 c. 1 lettera b) del GDPR]. Appare però necessario che tale formazione verta in particolar modo sui trattamenti effettivamente svolti dalle diverse unità organizzative in cui è articolata l'azienda. Si presenta un esempio di seminario orientato al personale che opera in una filiale bancaria.
Indice dell'intervento:

1. Importanza della formazione nella data protection: gli obblighi derivanti dal GDPR e da altri provvedimenti del Garante privacy.
2. Il ruolo del DPO e la relazione con la formazione sulla cybersecurity .
3. Un esempio concreto: la formazione per una filiale bancaria
    a. Inquadramento normativo e definizioni
    b. I principali adempimenti svolti in filiale: resa della informativa e raccolta del consenso.

Problematiche connesse: esercizio dei diritti da parte della clientela, marketing, accesso a dati bancari della clientela, disciplina delle comunicazioni alla clientela .

Relatore: ***Dott. Cesare Maria De Santis Puzzonia***
Ha lavorato per diverse aziende ed Enti - Ispettorato Telecomunicazioni e Assistenza al Volo dell'A.M., Ispettorato Logistico dell'A.M., Banca Nazionale del Lavoro, Ipacri SpA (Club sul Computer Crime), Istinform SpA, Euros Consulting SpA ed OASI SpA - prima di intraprendere un autonomo percorso professionale. Attualmente è amministratore unico di PRIMAe srl, società di consulenza operante sul tema della protezione dei dati personali ed è in possesso della certificazione CISM (Certified Information Security Manger) di ISACA ed iscritto altresì nel registro "Data Protection Officer", in accordo alla norma UNI 11697:2017, di KHC. Tra i clienti di PRIMAe srl si annoverano diverse società finanziarie e banche in alcune delle quali svolge il servizio DPO.

Con i consueti canali (mail, sito, numeri della Newsletter) vi informeremo delle prossime giornate di studio e dei seminari del nostro capitolo.

Gli annunci e gli inviti saranno spediti con le consuete modalità agli iscritti alla nostra mailing list.

I non iscritti possono ricevere tali comunicazioni inviando una mail con oggetto "subscribe" contenente solo nome e cognome a eventi<at>isacaroma.it

ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.

LE PRINCIPALI NOTIZIE

LE REGOLE DELL'INTELLIGENZA ARTIFICIALE

23 febbraio – Anche gli Stati Uniti si lanciano in un percorso di **regolamentazione sull'intelligenza artificiale**. E cominciano proponendo la versione 1.0 di un *Artificial Intelligence Risk Management Framework*, un sistema di indicazioni per la gestione dei rischi connessi alla produzione e all'utilizzo di intelligenza artificiale, prodotto dal *National Institute of Standards and Technology* (Nist) del Ministero del commercio.
Il Nist osserva che l'intelligenza artificiale pone rischi specifici e molto complessi da valutare.
(source: https://www.lasvolta.it/6334/le-regole-dellintelligenza-artificiale)

SPID A RISCHIO CHIUSURA AD APRILE? COSA SUCCEDERÀ ALL'IDENTITÀ DIGITALE

23 febbraio – Ad aprile 2023 scadono le convenzioni per la *gestione dello Spid*. Ad essere precisi, gli accordi sono scaduti a fine 2022, ma l'Agenzia per l'Italia digitale (Agid) li ha prorogati d'ufficio fino ad aprile. Il problema principale per i gestori sono i costi: le spese per i servizi di assistenza *ai 33 milioni di cittadini e alle 12 mila Pubbliche Amministrazioni che hanno adottato il sistema* sono ingenti e il governo non ha mai creato le condizioni per far sì che i privati adottassero lo Spid e creassero flussi di cassa per le aziende che gestiscono questo servizio.
(source: https://www.corriere.it/economia/lavoro/23_febbraio_23/spid-rischio-chiusura-ad-aprile-cosa-succedera-all-identita-digitale-fdb03c0a-b2aa-11ed-ab25-c6bbd9a5a3ea.shtml)

CYBERSECURITY: NUOVE TENDENZE NELLA FORMAZIONE

17 febbraio – Gli attacchi informatici evolvono continuamente nelle loro metodologie. Per questo motivo la formazione e l'aggiornamento del personale addetto alla sicurezza informatica deve far parte di ogni strategia aziendale che si rispetti. Oggi questo avviene anche con l'apprendimento autonomo, interattivo e su piccoli temi specifici come il phishing, la gestione delle mail, la tutela sulla privacy sui dati.
(source: https://www.avionews.it/it/item/1249555-cybersecurity-nuove-tendenze-nella-formazione.html)

LE PREOCCUPAZIONI DELL'INTELLIGENCE L'ATTACCO HACKER AI SITI ISTITUZIONALI CONTRO «L'ITALIA RUSSOFOBA»

23 febbraio – «Mamma mia». Poi un orso e la bandiera tricolore. La premier Giorgia Meloni aveva appena terminato la conferenza stampa congiunta a Kyjiv con il presidente Zelensky, e immediatamente sono partiti gli attacchi di hacker filorussi. Un gruppo che usa il nome collettivo "NoName057" ha tentato un attacco di tipo DDos (*Distributed Denial of Service*) – niente furto di dati, ma sistemi informatici mandati in tilt – contro i siti di enti pubblici e società private in Italia, tra banche, aziende e ministeri. Obiettivo dichiarato: «Smascherare l'Italia russofoba».
(source: https://www.linkiesta.it/2023/02/lattacco-hacker-noname057/)

L'INTELLIGENZA ARTIFICIALE È OVUNQUE, DAI MOTORI DI RICERCA ALLE LAMPADINE

21 febbraio – Quanti film abbiamo visto con protagonista l'intelligenza artificiale? E in quanti di questi le cose finivano malissimo? Tanti, ma per fortuna l'Intelligenza Artificiale di cui si parla in questi giorni non ha molto a che spartire con quelle assassine del grande schermo. Al momento, quella a cui possiamo accedere non ha coscienza, né autonomia di pensiero. Si limita a fare cose molto specialistiche, in ambiti limitati. Il suo utilizzo più diffuso è quello del riconoscimento vocale. Molti di noi hanno un assistente personale digitale a casa, tipo Alexa o Google Assistant, e quasi tutti ne portano uno in tasca, sia esso Assistant su Android o Siri sull'iPhone. Tutti usano l'IA, ma che cosa fanno?
(source: https://www.ilsole24ore.com/art/dai-motori-ricerca-lampadine-intelligenza-artificiale-e-ovunque-AEKqyQoC?refresh_ce)

DAL 1 AL 2 MARZO A ROMA CYBERSEC 2023, FOCUS SULLE ATTUALI SFIDE PER LA CYBERSICUREZZA

20 febbraio – Adolfo Urso, Ministro delle Imprese e del Made in Italy, Edmondo Cirielli, Vice Ministro Maeci, Alessio Butti, Sottosegretario alla Presidenza del Consiglio, Roberto Baldoni, Autorità Nazionale per la Cybersicurezza (Acn), Ivano Gabrielli, Direttore Polizia Postale e delle Comunicazioni, Alessandra Guidi, Vice Direttore Generale Dis, David van Weel, Assistant Secretary General for Emerging Security Challenges Nato, Mart Noorma, Director Nato Cooperative Cyber Defence Centre of Excellence (Ccdcoe) e Lorena Boix Alonso, Director for digital society, innovation and cybersecurity, Dg Connect, European Commission, sono alcuni dei 70 speaker di **CyberSec2023 - Nuovi Domìni, Guerre Ibride e Cooperazione**, la seconda edizione della Conferenza internazionale promossa ed organizzata dal quotidiano online Cybersecurity Italia. L'evento si terrà nei giorni 1 e 2 marzo a Roma, nella splendida cornice della 'Serra' del Palazzo delle Esposizioni, in via Milano 9/a. La conferenza, di cui l'Adnkronos è partner, si svolgerà prevalentemente in presenza, ma sarà possibile seguirla gratuitamente anche da remoto registrandosi su ***CyberSec2023***.
(source: https://www.adnkronos.com/dal-1-al-2-marzo-a-roma-cybersec-2023-focus-sulle-attuali-sfide-per-la-cybersicurezza_4HQ8wrNIQrRUfge1H9bhmZ)

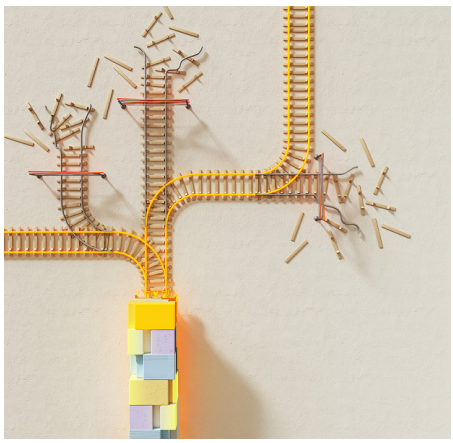
I 10 PUNTI ANCORA IRRISOLTI DEL REGOLAMENTO EUROPEO SULL'INTELLIGENZA ARTIFICIALE

ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.

26 febbraio – Dopo anni di negoziati, **entro il 2023 è prevista l'approvazione del regolamento dell'Unione europea** sull'*intelligenza artificiale*. Ma su molti punti dell'**Artificial Intelligence Act** (Ai Act) ancora non c'è accordo. Il Consiglio europeo ha **idee opposte** a quelle del Parlamento sul *riconoscimento facciale* in tempo reale, mentre all'interno dello stesso Europarlamento ci sono **posizioni contrastanti** sui *sistemi di identificazione delle emozioni*. Wired ha parlato con Brando Benifei, correlatore dell'Ai Act per l'Europarlamento e con Patrick Breyer, europarlamentare del Partito pirata tedesco, per identificare i **10 punti più controversi**, che saranno al centro dei **negoziati del trilogo**, ovvero le riunioni tra Parlamento, Consiglio e Commissione che dovranno trovare una mediazione.
(source: https://www.cybersecurity360.it/outlook/data-management-scopriamo-come-cambiera-nel-2023/)

IL FUTURO DELLA CYBERSECURITY NEGLI OSPEDALI

25 febbraio – Dall'inizio della **pandemia** ma anche con **l'invasione russa dell'Ucraina**, le strutture ospedaliere (così come i pazienti, i dati sanitari, i dispositivi medici) sono maggiormente esposte ai cyber attacchi. Con il Covid-19, infatti, la digitalizzazione ha assunto un ruolo sempre più centrale, basti pensare alle piattaforme di telemedicina oggi in uso e all'aumento delle soluzioni di smart working effettuato dal personale sanitario. In parallelo, il *Computer Security Incident Response Team* dell'**Agenzia per la Cybersicurezza Nazionale** ha ammonito che le aziende sanitarie e ospedaliere, "probabilmente in virtù degli aiuti umanitari che si stanno ponendo in essere", sono "obiettivo molto sensibile" di attacchi informatici. Invitandole, di conseguenza, ad "alzare al massimo i livelli di sicurezza", e a riporre "massima attenzione alla posta elettronica, all'antivirus, ai siti esposti verso l'esterno".



(source: https://trendsanita.it/il-futuro-della-cybersecurity-negli-ospedali/)

ANCHE IL GOVERNO ITALIANO VALUTA UN POSSIBILE BLOCCO DEL SOCIAL NETWORK CINESE TIK TOK

25 febbraio – L'applicazione del social network cinese Tik Tok è all'attenzione anche del governo italiano, dopo che dalla Commissione europea e dal Consiglio dell'Ue è arrivata la richiesta di disinstallarla a tutti i dipendenti, entro il prossimo 15 marzo. Nell'email inviata al personale Ue la richiesta era motivata dall'esigenza di "proteggere i dati della Commissione e aumentare la sua sicurezza informatica".
(source: https://www.rainews.it/articoli/2023/02/anche-il-governo-italiano-valuta-un-possibile-blocco-del-social-network-cinese-tik-tok-fc99e423-81de-45e3-905d-06a97fb06a72.html)

METAVERSO E CYBERSECURITY: COME DIFENDERSI DAI RISCHI?

24 febbraio – **Marco Fanuli, Security Engineer Team Leader di Check Point Software** riflette sul Metaverso e sulle sue vulnerabilità ed elenca le tre considerazioni principali legate alla sicurezza di questo mondo virtuale.
Dalle riunioni virtuali, alle customer experience immersive in 3D, fino ai tour panoramici di proprietà immobiliari, il Metaverso è destinato a trasformare il modo in cui le aziende operano. Secondo **Gartner**, entro il 2026, una persona su quattro passerà almeno un'ora del suo tempo nel Metaverso, per le motivazioni più diverse: lavoro, fare shopping, formazione, attività sui social media o semplice intrattenimento. Alcuni brand, come **Nike** e **Coca-Cola**, son già presenti e utilizzano questo mondo virtuale per migliorare la brand awareness e per spingere l'acquisto dei propri prodotti nel mondo reale.
(source https://www.bitmat.it/blog/internet/metaverso/metaverso-e-cybersecurity-come-difendersi-dai-rischi/)

CYBERSICUREZZA: VERSO L'AUTONOMIA STRATEGICA NAZIONALE

22 febbraio – La miglior difesa è l'attacco. Verso l'obiettivo della cyber immunità, attraverso l'autonomia strategica nazionale. La lotta verso il nemico strisciante dei sempre più frequenti attacchi informatici a Istituzioni e imprese sta cambiando passo. Soprattutto grazie all'Agenzia per la Cybersicurezza Nazionale, che ha organizzato a Roma in collaborazione con l'Università Luiss Guido Carli l'evento "Il cantiere della cybersicurezza: sviluppo tecnologico ed autonomia strategica nazionale". Hanno partecipato il ministro delle Imprese e del Made in Italy, **Adolfo Urso**, il sottosegretario di Stato alla Presidenza del Consiglio e Autorità delegata alla sicurezza della Repubblica, **Alfredo Mantovano**, e il Direttore Generale dell'Agenzia per la Cybersicurezza Nazionale, Prof. **Roberto Baldoni**. L'iniziativa rientra negli 82 obiettivi previsti entro il 2026 dalla Strategia Nazionale di Cybersicurezza, al fine di promuovere la ricerca e l'innovazione nel settore della cybersicurezza, potenziare l'autonomia strategica nazionale e sostenere lo sviluppo di capacità tecnologiche nazionali ed europee.
(source: https://www.thewatcherpost.it/top-news/cybersicurezza-verso-lautonomia-strategica-nazionale/)

CYBERSICUREZZA: QUALE RUOLO PER GLI ITS NELLA FORMAZIONE

23 febbraio – Lo scorso 5 febbraio un **massiccio attacco hacker** *ha colpito* molti sistemi informatici in tutto il mondo, **Italia inclusa**. L'**Agenzia per la cybersicurezza nazionale** (Acn), l'autorità che si occupa di implementare la strategia nazionale di cybersicurezza, *ha rilevato* come siano state "*decine le realtà che hanno riscontrato l'attività malevola nei loro confronti*". I recenti fatti hanno in qualche modo riacceso i riflettori su un tema: **la formazione sul contrasto agli attacchi informatici**. Un tipo di formazione su cui gli **ITS Academy** possono giocare un ruolo importante.
(source: https://tuttoits.it/cybersicurezza-ruolo-its-formazione/)

ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.

CORSI ISACA

L'ATTIVITÀ FORMATIVA DI ISACA ROMA NON È SOSPESA!
I CORSI SONO EROGATI IN MODALITÀ ONLINE

LA NUOVA CERTIFICAZIONE CSX-P (CYBERSECURITY PRACTITIONER)

Per ulteriori informazioni visitare il sito dedicato alla certificazione CSX-P (www.csxp.it).

ULTERIORI INFORMAZIONI SUI CORSI NELLE SEZIONI SPECIFICHE DEL SITO WWW.ISACAROMA.IT

Cybersecurity Nexus (CSX) è il programma professionale di ISACA Intl con il quale verranno sviluppate le conoscenze per una corretta gestione della sicurezza informatica. Il programma CSX è il risultato dell'esperienza ultradecennale maturata da ISACA Intl nelle attività di auditing, di gestione dei rischi, del security management e dell'IT governance. CSX sta aiutando a plasmare il futuro della sicurezza informatica.

INFORMAZIONI UTILI

Chi ha già frequentato un corso a pagamento presso ISACA Roma ha uno sconto del 10%. Aziende, grossi enti, PAL, PAC e Difesa possono richiedere i costi a loro riservati alla casella **corsi<at>isacaroma<dot>it**
Per ulteriori informazioni sui corsi inviare una mail all'indirizzo: **corsi<at>isacaroma<dot>it**

Info e Contatti

info@isacaroma.it

Via Berna, 25 - 00144 Roma

Social Media

http://www.isacaroma.it/

SAPIENZA
UNIVERSITÀ DI ROMA

ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.

CISA, CRISC, CISM, CGEIT, CSX-P O CDPSE
DOPO IL TUO NOME DIMOSTRA CHE HAI LE COMPETENZE PER AFFRONTARE LE SFIDE DELL'AZIENDA MODERNA:

GET CERTIFIED

Info al sito *https://www.isaca.org/credentialing/*

Questa Newsletter è indirizzata ai soci del Capitolo di Roma di ISACA e viene anche spedita alle persone che hanno chiesto di essere inseriti nella mailing list per la comunicazione degli eventi del Capitolo.
Potete indirizzare ogni vostra richiesta (commenti, contributi, cancellazione dalla lista, ecc.) a newsletter<at>isacaroma.it.
La redazione della Newsletter è curata da Mario Taddonio (membro del CD di ISACA Roma) m.taddonio<at>isacaroma.it e da Glauco Bertocchi (VicePresidente di ISACA Roma) g.bertocchi<at>isacaroma.it
Le opinioni espresse (editoriale, ecc.) rappresentano quelle dei rispettivi autori.

ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.